

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO**

In the Matter of the Search of:)	No. 2:25-mj-139
)	
The digital device that is listed in Attachment A that were obtained from Phillip Wiseman and which are currently in the custody of the Perry County Sheriff's office in Perry County, Ohio.)	Magistrate Judge
)	
)	<u>UNDER SEAL</u>

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jeremy Lindauer (Your Affiant), a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with the Federal Bureau of Investigations (FBI) and have been since September of 2015. I am currently assigned to the Resident Agency in Athens, Ohio. Prior to joining the FBI, I worked as a patrol officer for the Fishers Police Department in Fishers, Indiana, between 2008 and 2015. While there, I received training and experience in conducting many types of criminal investigations, including crimes against children. I was promoted to Field Training Officer for the department prior to leaving to accept a position as Special Agent for the FBI in 2015.
2. Within the FBI, I was first assigned to the Joint Terrorism Task Force in New York City, where I conducted and assisted in complex terrorism investigations across the globe. I was transferred to the Athens Resident Agency in September of 2020, where my responsibilities expanded to include investigating criminal violations relating to child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.
3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

5. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachments A and B** of this Affidavit. The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for a search warrant for the mobile devices including a white HP all-in-one desktop computer, Model Number 24-DD0010, Serial Number 20WW1ZET60 and a black Samsung Galaxy A13 5G cellular phone, serial number R5CT925NG5V, and IMEI 357161671539376, both of which are located at the Perry County Sheriff's Office at 5720 State RT 345, New Lexington, OH 43764 (collectively the **SUBJECT DEVICES**).
6. The **SUBJECT DEVICES** to be searched is more particularly described in **Attachment A**, for the items specified in **Attachment B**, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – the sexual exploitation of a minor and the advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter “child pornography”), distribution, transmission, receipt, and/or possession of child pornography, as well as the coercion or enticement of a minor(s). I am requesting authority to seize and examine the **SUBJECT DEVICES**, for items specified in **Attachment B**, and to seize all items listed in **Attachment B** as evidence, fruits, and instrumentalities of the above violations.

APPLICABLE STATUTES AND DEFINITIONS

7. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to

know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

8. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.
9. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
10. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that

has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

11. Title 18, United States Code, Section 2422(b), makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime. Production of child pornography as defined in 18 U.S.C. § 2251(a) is included in the definition of sexual activity for which any person may be charged with a crime.
12. As it is used in 18 U.S.C. §§ 2251 and 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.
13. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
14. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i)

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and all Attachments hereto include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

- bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.
15. The term “minor”, as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as “any person under the age of eighteen years.”
 16. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”
 17. The term “visual depiction,” as used herein, is defined pursuant to 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
 18. The term “computer”² is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
 19. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

² The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

20. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.
21. Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
22. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
23. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BACKGROUND REGARDING THE INTERNET AND MOBILE APPLICATIONS

24. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of

electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

25. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
26. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.
27. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.
28. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very

high resolution. Tablet devices have average storage capabilities ranging from 16 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

29. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records

may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.

30. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography, or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
31. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
32. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of

- an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
33. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
34. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.
35. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include Facebook Messenger, Snapchat, X (formerly known as Twitter), and Instagram.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

36. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
 - b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
37. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).
38. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

39. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in **Attachment B**;
 - b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in **Attachment B**;
 - c. Surveying various files, directories and the individual files they contain;
 - d. Opening files in order to determine their contents;
 - e. Scanning storage areas;
 - f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or
 - g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

INVESTIGATION AND PROBABLE CAUSE

40. On or about November 11, 2023, the Perry County Sheriff's Office (PCSO) received a call from a private organization called Predator Poachers (PP). PP is a group that identifies themselves as investigative journalists, and they conduct their investigations by placing "decoy" accounts on social media applications such as Facebook. The PP decoy accounts are utilized by PP adult members who pose as minors. If and when these decoys communicate with individuals who indicate they are interested in sexual relationships with the decoy, PP sets up a meeting where the decoy can present him/herself as a minor and determine who the subject is and what their intentions were with the child.
41. Upon receiving the call, PCSO learned that PP had a total of four individuals participating in an investigation in the area of Zanesville and Crooksville, Ohio.
42. On the evening of November 11, 2023, notified PCSO that they had confronted a man named Phillip WISEMAN who had met their decoy at an apartment in Zanesville, OH with

the implied intention to have sexual contact with the decoy. Throughout the communications PP had with WISEMAN, their decoy had explicitly stated to WISEMAN that she was 11 years old. PP informed PCSO that after WISEMAN was told the person he was communicating with was an 11-year-old female, WISEMAN sent two unsolicited videos depicting child pornography to the decoy.

43. PCSO learned that the PP group arranged a meeting location with WISEMAN at an apartment in Zanesville, Ohio. When WISEMAN arrived at the Zanesville apartment he met up with the decoy, who was an adult member of PP but extremely young looking. WISEMAN was then confronted by other members of the PP group and made admissions about sending child pornography to the decoy and generally described the types of videos he had as depicting minor females dancing naked or engaged in sex acts with adult males. WISEMAN also admitted to having up to fifty child pornography files on his computer at his house.
44. After learning about WISEMAN's computer, the PP group requested to meet WISEMAN at his residence and WISEMAN agreed, providing them the address of where he lived: 222 McKee Street in Crooksville, Ohio. The PP group then traveled separately from WISEMAN to WISEMAN's home and stood by until police arrived.
45. After receiving a call related to this incident, PCSO was dispatched to the residence of WISEMAN and, upon arriving on scene, spoke with multiple PP members outside. PCSO then knocked on WISEMAN's front door and obtained verbal permission to enter from a female, now known to be a family member of WISEMAN, who also resided with WISEMAN at 222 McKee Street.
46. Upon entering into the residence, PCSO observed WISEMAN sitting in a chair in front of a computer. PCSO then spoke with WISEMAN and asked if he had child pornography on his computer and WISEMAN confirmed he did. Law enforcement asked if WISEMAN knew that was illegal, and WISEMAN stated that he did know it was illegal and it was stupid to keep the files. WISEMAN then showed law enforcement the file location on his computer where he kept child pornography content. That device was one of the **SUBJECT DEVICES**, specifically the white HP All-In-One desktop computer.
47. After learning about the content contained on the desktop computer, WISEMAN was informed that the computer needed to be seized. WISEMAN was then placed in handcuffs

and informed that he was being detained. PCSO subsequently placed WISEMAN into a police vehicle and seized his desktop computer as well as his Samsung Galaxy A13 cellular phone, the other **SUBJECT DEVICE**, which was located on the same desk as the HP All-In-One computer. Prior to his detention WISEMAN showed PCSO this cell phone and identified it as his own.

48. After both **SUBJECT DEVICES** were seized, PCSO spoke with WISEMAN and provided him his *Miranda* warnings. WISEMAN agreed to speak to PCSO and admitted to communicating with the decoy who told him she was 11 years old. WISEMAN clarified that he believed the female he was speaking with was possibly 15 years old because that's what it said on her Twitter account. WISEMAN stated that he sent her pictures of himself including pictures of his penis. WISEMAN also admitted that he had pictures and videos of child pornography on the desktop computer which had been sent to him. WISEMAN denied ever creating child pornography himself.
49. PCSO then asked WISEMAN if he was willing to consent to a search of the **SUBJECT DEVICES**, and if he would sign a consent to search form. WISEMAN agreed and said they could do anything they want. WISEMAN was then transported to the PCSO for the purpose of completing a consent to search form for both the **SUBJECT DEVICES**. WISEMAN was not in handcuffs at the time of the consent and was sitting in a room inside the PCSO. WISEMAN read the terms of the consent form out loud prior to signing and then freely signed the forms. This interaction was audio and video recorded, and a copy of the recording is maintained by the PCSO. WISEMAN was then transported back to his home and released.
50. On or about March 28, 2024, the **SUBJECT DEVICES** were sent to the Ohio Bureau of Criminal Investigation (BCI) Cyber Crimes Division to conduct the search. On or about August 7, 2024, agents with BCI conducted the search and identified multiple images and videos of potential child pornography. A report was then sent to PCSO which was reviewed by them in September 2024.
51. In January 2025, law enforcement with PCSO reviewed the potential child pornography identified by BCI, beginning with the Samsung Galaxy cellular phone. Multiple videos of an approximately five-year-old minor female (herein after Minor Victim One), believed to be a family member of WISEMAN, were observed. In the videos, Minor Victim One was

observed taking videos of herself while fully nude. Law enforcement noted that in one video, the camera view panned around the room and showed WISEMAN sitting at his computer while his granddaughter was naked on the couch taking the video. Other images of unknown minor females displaying their breasts and vaginas were also noted.

52. Law enforcement then reviewed some of the contents of the desktop computer and discovered multiple photographs of unknown minor females in various positions or states of nudity, displaying their genitals, or engaged in sexual acts. PCSO then contacted FBI Cincinnati Division, Athens RA for further assistance conducting the investigation and analyzing the content of the **SUBJECT DEVICES**.
53. Based on the foregoing, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – sexual exploitation of a minor, advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter “child pornography”), distribution, transmission, receipt, and/or possession of child pornography, as well as the coercion or enticement of a minor(s) had been committed or were about to be committed, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, are located on/in the **SUBJECT DEVICES**.
54. Therefore, I respectfully request that this Court issue search warrants for the device described in **Attachment A**, authorizing the seizure and search of the items described in **Attachment B**.

**COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL
INTEREST IN CHILDREN**

55. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in communicating about and engaging in sexual abuse of children
- a. Those who communicate about and engage in sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses,

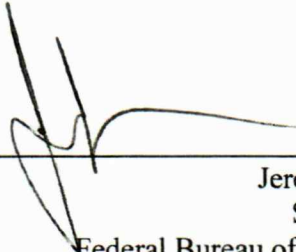
such as in person, in photographs, or other visual media; or from literature and communications about such activity.

- b. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography sometimes maintain any "hard copies" of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections and communications are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- d. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- e. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.
56. Based upon the conduct of individuals involved in seeking/soliciting, creating, receiving, distributing, and/or collecting child pornography set forth in the above paragraphs, and the facts learned during the investigation in this case, namely, that WISEMAN traveled to an apartment to meet a purported 11-year-old female for sex, and had nude images of minor children, including his own family member, on his devices, your affiant has reason to believe that WISEMAN has a sexual interest in minors and has viewed or sought out visual depictions of minors engaged in sexually explicit conduct utilizing an internet-capable device. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – sexual exploitation of a minor, advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter “child pornography”), distribution, transmission, receipt, and/or possession of child pornography, as well as the coercion or enticement of a minor(s) will be located on the **SUBJECT DEVICES**.

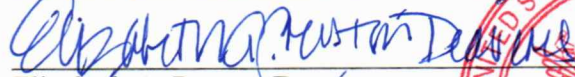
CONCLUSION

57. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – sexual exploitation of a minor, advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter “child pornography”), distribution, transmission, receipt, and/or possession of child pornography, as well as the coercion or enticement of a minor(s), have been committed, and evidence of those violations is located on the **SUBJECT DEVICES** described in Attachment A. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the **SUBJECT DEVICES** described in Attachment A.



Jeremy Lindauer
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 12th day of March, 2025.



Elizabeth A. Preston Deavers
United States Magistrate Judge
United States District Court
Southern District of Ohio

